We claim:

1. A consumable authentication protocol for validating the authenticity of an untrusted authentication chip, the protocol includes the steps of:

generating a random number and applying an asymmetric encrypt function to the random number using a first key to produce a first outcome;

passing the first outcome to the untrusted authentication chip;

decrypting the first outcome with an asymmetric decrypt function using a secret key to produce a second outcome, in the untrusted chip;

applying the asymmetric encrypt function to the second outcome together with a data message read from the untrusted chip using the secret key to produce a third outcome, in the untrusted chip;

receiving the third outcome together with the data message;

decrypting the third outcome and comparing the decrypted random number and data message with the generated random number and the received data message;

in the event of a match, considering the untrusted chip and the data message to be valid;

otherwise considering the untrusted chip and the data message to be invalid.

2. A consumable authentication protocol according to claim 1, for validating the authenticity of an untrusted authentication chip, as well as ensuring that the authentication chip, lasts only as long as the consumable including the further steps of writing new data to the untrusted chip, performing the steps of claim 1, and in the event the untrusted chip is found to be authentic and the new data is the same as the data message read from the untrusted chip, then the write is validated.

3. A consumable authentication protocol according to claim 1, where the first key is a public key.

4. A consumable authentication protocol according to claim 1, where encryption outside the untrusted chip is implemented in software

5. A consumable authentication protocol according to claim 4, where the random number generation, encryption, passing, and final decrypting and comparing steps take place in an external system.

6. A consumable authentication protocol according to claim 5, where the external system is in a printer or other device in which consumables such as ink cartridges are mounted.

7. A consumable authentication protocol according to claim 6, where the untrusted chip is in the consumable.

8. A consumable authentication protocol according to claim 1, where the encryption outside the untrusted chip is implemented in a second authentication chip, and an external system intermediates between the two chips.

9. A consumable authentication protocol according to claim 8, where the second authentication chip and system are in a printer or other device in which consumables are mounted.

10. A consumable authentication protocol according to claim 9, where the untrusted chip is in the consumable.

11. A consumable authentication protocol according to claim 1, where the secret key is held only by the untrusted chip.

12. A consumable authentication protocol according to claim 1, where the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every successful authentication so that the next random number will be produced from a different seed.

13. A consumable authentication protocol according to claim 1, where the data message is a memory vector of the authentication chip, a part is different for each chip, and parts of it are constant (read only) for each consumable, or decrement only so that it can be completely downcounted only once for each consumable.

14. A consumable authentication system for performing the method according to claim 1; where the system includes a random number generator, an asymmetric encryptor to encrypt generated random numbers with an asymmetric encryption function to produce a first outcome and a first key for the encryptor, a test function and an untrusted authentication chip; the untrusted chip includes a read function which operates to decrypt the first outcome using a secret key and produce a second outcome, then applies the symmetric encrypt function to the second outcome together with a data message read using the secret key to produce a third outcome, it also returns the third outcome together with the data message in the clear; the test function operates to decrypt the third outcome and compare the decrypted second outcome and data message with the generated random number and the clear data message; in the event of a match the test function returns a value indicating validity; otherwise it returns a value indicating invalidity.

15. A consumable authentication system according to claim 14, where new data written to the untrusted chip is considered valid in the event the untrusted chip is found to be authentic and the new data is the same as the data message read from the untrusted chip.

16. A consumable authentication system according to claim 14, where the first key is a public key.

17. A consumable authentication system according to claim 14, where encryption outside the untrusted chip is implemented in software

18. A consumable authentication system according to claim 17, where the random number generation, encryption, passing, and final decrypting and comparing steps take place in an external system.

19. A consumable authentication system according to claim 18, where the external system is in a printer or other device in which consumables such as ink cartridges are mounted.

20. A consumable authentication system according to claim 19, where the untrusted chip is in the consumable.

21. A consumable authentication system according to claim 14, where the encryption outside the untrusted chip is implemented in a second authentication chip, and an external system intermediates between the two chips.

22. A consumable authentication system according to claim 21, where the second authentication chip and system are in a printer or other device in which consumables are mounted.

23. A consumable authentication system according to claim 22, where the untrusted chip is in the consumable.

24. A consumable authentication system according to claim 14, where the secret key is held only by the untrusted chip.

25. A consumable authentication system according to claim 14, where the random number generator of the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every successful authentication so that the next random number will be produced from a new seed.

26. A consumable authentication system according to claim 25 where for a group of authentication chips, the initial seed for each chip is different from that of the others in the group so that the first random number produced by each chip in the group will be different.

27. A consumable authentication system according to claim 14, where the data message is a memory vector of the authentication chip, a part is different for each chip, and parts of it are constant (read only) for each consumable, or decrement only so that it can be completely downcounted only once for each consumable.